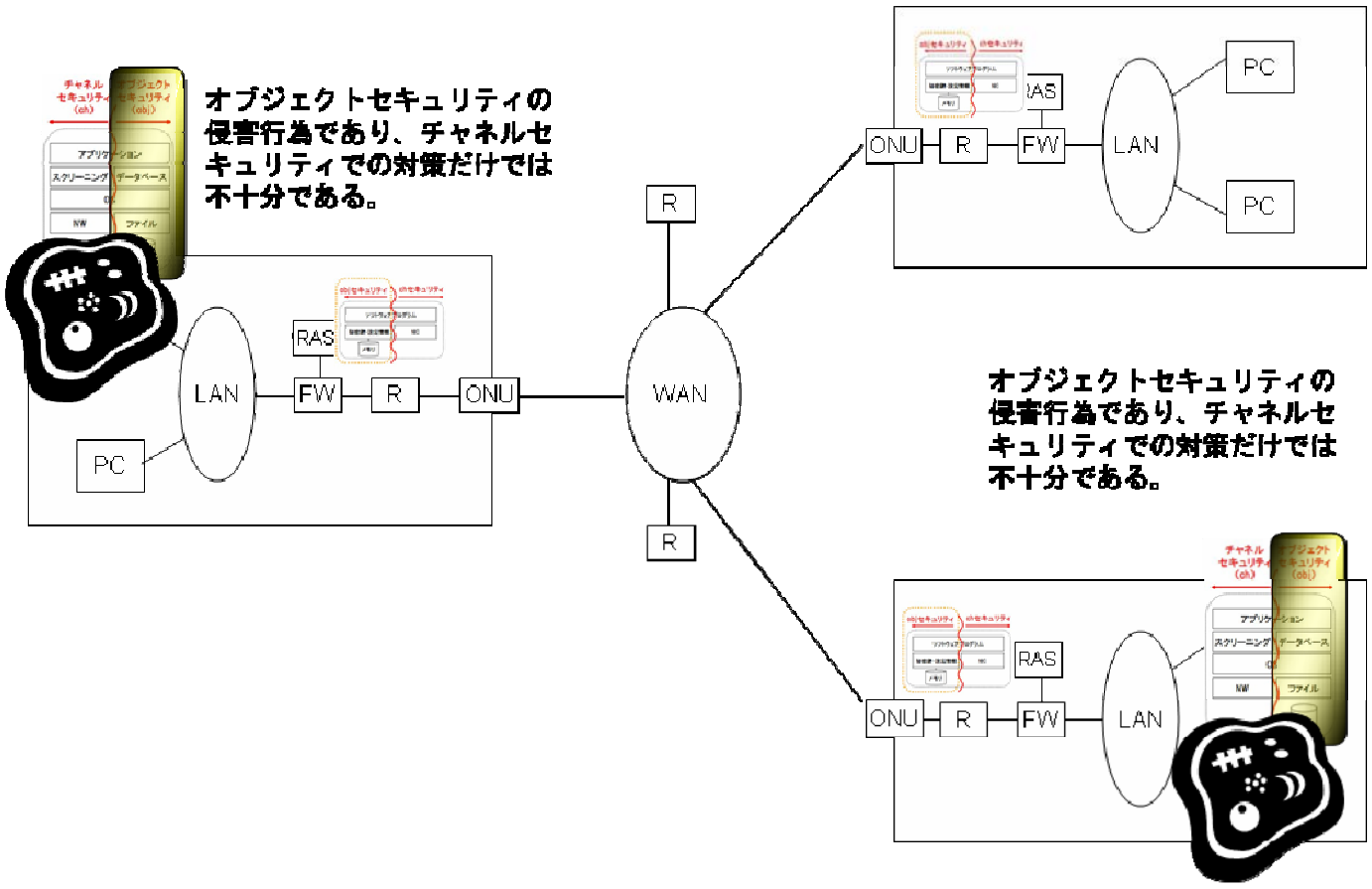
項番	T10. 情報の不正コピー	脅威の大区分	盗聴	守るべき資産	ソフトウェアプログラム（オブジェクトセキュリティ）	対象	AP/NW
解説	ウイルスには、特定の日になると、というような特定の条件のもとでのみ動作する「時限爆弾」があり、特定の関連したプログラムが動作しない限り、システム中に隠れているものも存在する。さらに常時動作しており、危害を加える期をうかがっているものもある。また巧妙なウイルスには、単にシステムの設定を変更したり、隠れてしまうものもある。(RFC2504)						
対策の概要							

脅威発生のイメージ



＜対策の概要＞

オブジェクトセキュリティの侵害行為であり、チャネルセキュリティでの対策だけでは不十分である。

加えて、ネットワーク機器のオブジェクトセキュリティでの対策としても検討すべきである。

脅威の内容	$ virus （ウイルス） (I) 他のプログラムに感染すること（すなわち、自身の複製を挿入し、その一部となること）によって広める、隠れた、コンピュータ ソフトウェアの自己増殖部分であり、通常、悪意あるロジック。ウイルスは、自身では動作することができない。; ウイルスは、その宿主プログラムが、そのウイルスを活動させるために動作させられることを必要とする。

対策				リスク	
対策の内容	参照文書	対策表との対比 方法	対策表との対比 有効度	頻度	影響度
あなたのシステムに、どんなソフトウェアをインストールするかについて慎重であってください。	RFC2504				
できるならば「信頼できる入手元」からのソフトウェアを使用してください。	RFC2504				
いかなるソフトウェアをインストールするときにも、その前にあなたのサイトのポリシーをチェックして下さい。	RFC2504				
サイトによっては、セキュリティやシステム保守問題を避けるために、管理者にのみソフトウェアのインストールを許可しています。	RFC2504				
集中管理されたサイトには、ウイルスの脅威を扱うためのポリシーやツールがあります。あなたのサイトポリシーにあたるか、もしくは、あなたのシステム管理者からウイルス問題を解消する正しい手順を聞き出してください。	RFC2504				
ウイルス検出ツールが、あなたのシステムの問題があることを示している場合、それを報告する必要があります。	RFC2504				
あなたにそのウイルスを渡したと思われる人にだけでなく、あなたのサイトのシステム管理者にも通知する必要があります。	RFC2504				
平静であることが重要です。	RFC2504				
ウイルスに脅えることは、実際のウイルス発生 以上の遅れや混乱を引き起こします。	RFC2504				
根絶のプロセスにおいて、ウイルス対策ソフトウエアのような、それを助けてくれる ソフトウエアが入手可能です。	RFC2504				
ウイルスについて広くアナウンスする前に、ウイルス検出ツールを使用して、できれば技術的能力のある人物の支援のもと、その存在を確認するようにしてください。	RFC2196				
もし、何らかの偽造ファイルが作成されていたら、それらを削除する前に アーカイブにして下さい。	RFC2196				
ウイルス感染の場合、感染したファイルを含むすべてのメディアについて駆除や 再フォーマットを行うことが重要です。	RFC2196				
最後に、すべてのバックアップがクリーンであることを確認してください。	RFC2196				
ウイルスに感染した多くのシステムが、周期的に再度感染するのは、単に体系的に ウイルスをバックアップから撲滅していないからです。根絶した後、新たにバックアップが採られる必要があります。	RFC2196				